

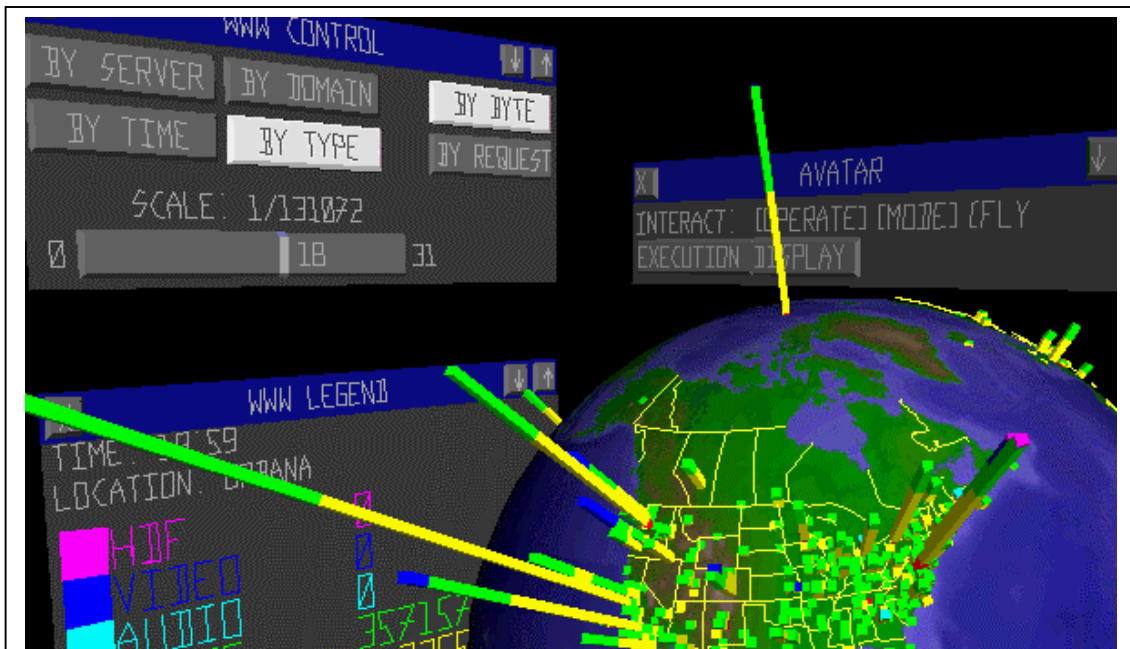
# Cyberspace Situational Awareness Demands Mimic Traditional Command Requirements

*Experience gained from battlefields helps military prepare information operation defenses.*

By Tim Bass

Next-generation network management and intrusion detection systems will fuse data, combining both short-term sensor data with long-term knowledge databases to provide cyberspace situational awareness-based decision support systems and cyberspace command and control. Sophisticated computer hardware and software will identify a myriad of objects against a noise-saturated environment. Cyberspace command and control systems will track the objects, calculate the velocity, estimate the projected threats and provide other critical decision support functions.

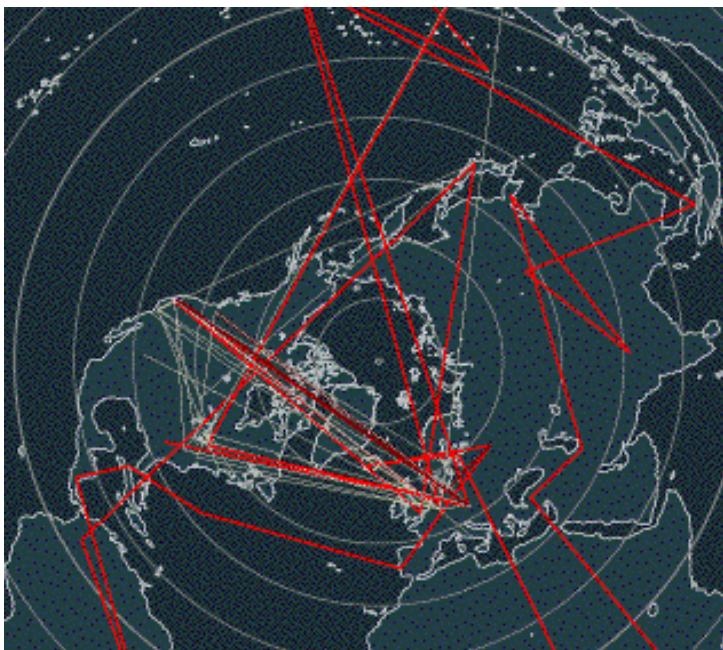
Numerous constructs currently used to monitor and control objects in traditional airspace apply to monitoring information-based objects in data networks. These concepts are evolutionarily similar to the situational awareness required in current-generation air traffic control. Lt. Col. David Gruber, Communications Squadron Commander, Hickam Air Force Base, Hawaii, is convinced that an analogous fusion paradigm is required between network management, Internet traffic control and future intrusion detection systems if U.S. military organizations are to maintain information superiority in cyberspace.



University of Illinois researchers created a graphic depiction of cyberspace command and control. The size of the globe and the height of the data bars are controlled by sliders. The globe can be rotated at various speeds.

This new globally reachable battlespace has some unique warfare characteristics, as recently discussed by U.S.A.F. Brig. Gen. Dale W. Meyerrose, Director of Communications and Information Systems, Headquarters Air Combat Command, Langley Air Force Base. In traditional air and space warfare, the air and space media for operations and deployment are natural resources that do not have to be created nor maintained by the warfighter. In elementary terms, it is simply not necessary to create and sustain the air and space in which forces traditionally operate.

Cyberspace and critical electronic infrastructures, on the other hand, must be artificially created and sustained before information operations occur. Because information operations in cyberspace takes place in an artificially created medium, the doctrine of cyberwarfare is much different than traditional warfare, which occurs in a natural media for transportation and deployment. Officials at Langley AFB have implemented initiatives to examine how the concept of creating and sustaining information infrastructures will effect future U.S. Air Force doctrine. Network communications has evolved from a subordinal operational support function to a major warfighting element with unique doctrine and operational constructs. In global information operations, the communications organization creates and maintains the air in which information flies.



**University of Illinois -Urbana-Champaign software *ip2ll* maps IP address space to longitude and latitude for global Internet network traffic. The database mapping, used to create this visualization, is one example of the long-term knowledge necessary for cyberspace command and control systems.**

In a typical command and control (C2) system, sensors observe electromagnetic radiation, acoustic noise, thermal energy, nuclear particles, infrared radiation, and other signals. Cyberspace C2 (CC2) systems have different sensors and constructs because the environment has changed. Instead of a missile launch and supersonic transport through the atmosphere, cyberspace sensors observe information flowing in networks. Yet, just as C2 operational personnel are interested in the origin, velocity, threat and targets of a warhead, CC2 personnel are concerned about the identity, rate of attacks, threats and targets of both friendly and hostile information objects in cyberspace.

The inputs into CC2 fusion systems will consist of sensor data, commands and *a priori* data from established long-term and short-term knowledge centers. For example, the CC2 system input would be information from numerous distributed packet sniffers, system log-files, Simple Network Management Protocol (SNMP) traps and queries, signature-based intrusion detection systems, user profile databases, system messages, threat databases and operator commands. Traditional signature-based network intrusion detection will perform an architectural role similar to signature-based antiviral software

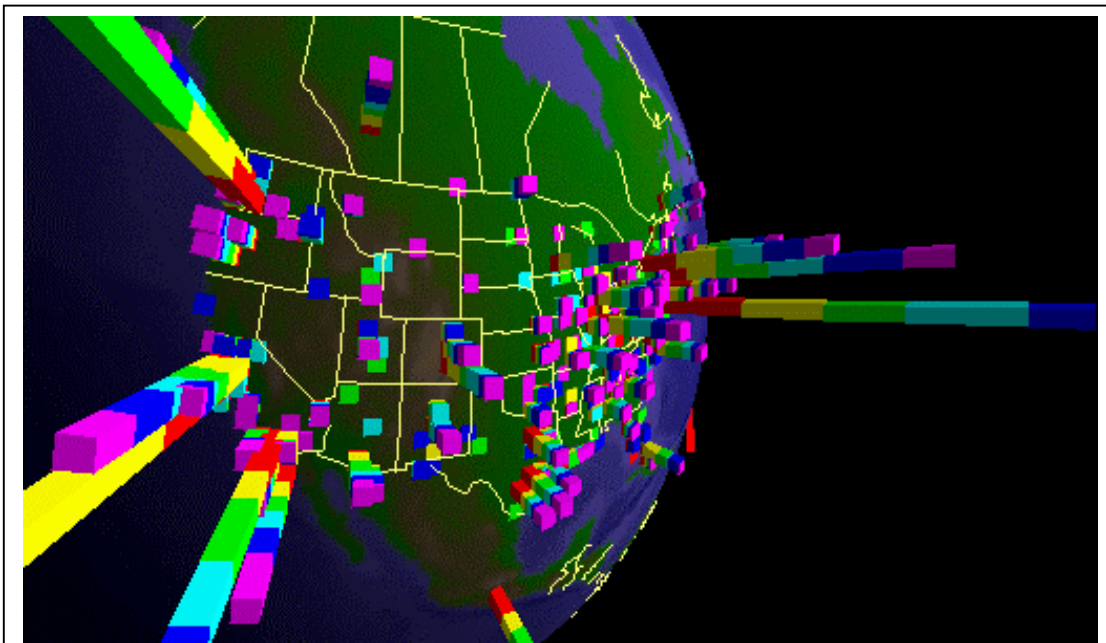
Visualization of attack scenarios is considered to be critical for future CC2 decision-makers. The figures in this article represent future CC2 decision support systems created by researchers at the University of Illinois. These examples represent the possible outputs of future CC2 systems, illustrating virtual reality-based global WWW traffic analysis and a geographic mapping of network-based attacks in the Internet. In one example from the *ip2ll* server project, a database containing long-term knowledge of the relationship of IP addresses to geographic space is used to visualize global Internet data flows. Mapping cyberspace to geographic space is critical to decision makers in these visualizations.

The output of fusion-based CC2 systems are estimates of the identity (and possibly the location) of a threat source, the malicious activity, taxonomy of the threats, the attack rates, and an assessment of the potential severity of the projected target and CC2 decision support visualizations and simulations. Numerous C2 constructs map directly to future CC2 systems. The detection performance of a CC2 sensor is the detection characteristic, including the false alarm rate, detection probabilities and ranges, for the information-object of interest tracked against a network-centric noise background. For example, when detecting malicious activity, non-malicious activity will be modeled as noise.

The CC2 sensor capability to distinguish between two or more network-centric objects in space or time is the spatial and temporal resolution. The spatial coverage is the span, or field of view, of the sensor. For example, the spatial coverage of a system log file is the computer system processes and system calls being monitored. The mode of operation of the sensors, scanning, single, or multiple network object capability, is important for CC2 sensor classification and system integration. C2 concepts apply to the CC2 target revisit rate, the measurement accuracy, and information-object measurement dimensionally. Hard and soft CC2 sensor reporting characteristics refer to the decision status of cyberspace sensor reports. Commanders need to know if a critical operational decision can be made without sensor correlation; or does the CC2 sensor require confirmation?

For effective CC2, situational data is collected from numerous network objects with elementary observation primitives including information-object identifiers, times of observations and other technical attributes. Every network device and object has the potential to be used as a CC2 sensor providing both low-level data and refined information to CC2 distributed processors. Current-generation intrusion detection systems rely on in-band processing, which can only achieve limited temporal resolution. Out-of-band CC2 networks will be required for extremely critical real-time systems.

The Defense Advanced Research Projects Agency (DARPA) has recently started examining next-generation information CC2 systems. DARPA's future information assurance vision is a strategic cyberspace decision support system that enables leaders to understand strategic network situations and react quickly to these situations. CC2 decision support envisioned by DARPA is intended to provide battle management over systems under attack by adversaries seeking to achieve strategic goals by assisting users to understand the activities and objectives of adversaries operating within network environment. Increased confidence and situational awareness provides the foundation for determining the most effective courses of action to counter future hostile activities in the emerging network-centric battle and information spaces.



**The real-time geographic visualization of World Wide Web Traffic, designed by Stephen E. Lamm and Daniel A. Reed of the University of Illinois-Urbana-Champaign and Will H. Scullin of Netscape Communications Corporation, is an example of the fusion of geographic space and network traffic parameters and characteristics. Data Bar with data bars represent attributes such as document type, Internet domains, services or time delays.**

## *AFCEA Signal Magazine, February 2000*

The emerging DARPA research initiatives will help prepare the U.S. to develop a more comprehensive understanding of cyberspace command and control operations as the military creates, deploys and flies missions in globally connected networks. Nationwide experts gathered at a joint Department of Energy, National Security Council and Office of Science and Technology workshop concluded that commercial off-the-shelf products are dramatically behind the power curve in situational and visual command and control support tools. DARPA and the DoE workshop participants concluded that it is critical for the U.S. to clearly define the underlying scientific and technical constructs of internal cyberspace command and control operations before funding large CC2 programs.

### Internet Resources

Topic	URL
CC2 Papers	<a href="http://www.silkroad.com/papers/published.html">http://www.silkroad.com/papers/published.html</a>
WWW	<a href="http://vibes.cs.uiuc.edu/Project/VR/WWW/WWWPaper.htm">http://vibes.cs.uiuc.edu/Project/VR/WWW/WWWPaper.htm</a>
Visualization	
IP2LL	<a href="http://www-unix.mcs.anl.gov/~olson/IPtoLL.html">http://www-unix.mcs.anl.gov/~olson/IPtoLL.html</a>
DARPA CC2 BAA	<a href="http://web-ext2.darpa.mil/iso/ia&amp;s/IASPIP990811Final.html">http://web-ext2.darpa.mil/iso/ia&amp;s/IASPIP990811Final.html</a>

CC2 systems that provide long-term threat, countermeasure and other security-related information to fusion systems are emerging as critical scientific research and development areas. Cyberspace situational awareness is required to operate and survive in complex global network infrastructures where both friendly and hostile activities coexist. According to Lt. Col. David Uhrich, Chief of Network Plans, HQ ACC, Langley. AFB, Virginia, current-generation intrusion detection technologies are inadequate. Future cyberspace rules-of-engagement doctrines depend on the timeliness, fidelity and accuracy of CC2-based knowledge. These emerging requirements require highly sophisticated cyberspace decision support systems in order for U.S. forces to maintain information superiority, he says.

---

**Tim Bass** is the President of **Silk Road** [WWW.SILKROAD.COM](http://WWW.SILKROAD.COM). Mr. Bass [BASS@SILKROAD.COM](mailto:BASS@SILKROAD.COM) provides network-centric subject matter expertise to Headquarters Air Force (USAF/SC), the U.S. Department of Energy, and multinational financial institutions.